UNITED STATES PATENT AND TRADEMARK OFFICE

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/849,099	05/04/2001	Praerit Garg	MSFT-0223/158385.1	7971

7590	12/21/2004

WOODCOCK WASHBURN KURTZ
MACKIEWICZ & NORRIS LLP
One Liberty Place -46th Floor
Philadelphia, PA 19103

EXAMINER
LEMMA, SAMSON B

ART UNIT	PAPER NUMBER
2132	

DATE MAILED: 12/21/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

	Application No.	Applicant(s)
Office Action Summary	09/849,099	GARG ET AL.
	Examiner	**Art Unit**	
	Samson B Lemma	2132	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE <u>3</u> MONTH(S) FROM
THE MAILING DATE OF THIS COMMUNICATION.
- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed
  after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
  Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any
  earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on <u>04 May 2001</u>.

2a)☐ This action is **FINAL**.   2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is
     closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) <u>1-21</u> is/are pending in the application.

     4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) <u>1-21</u> is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

     Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

     Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

     a)☐ All   b)☐ Some *   c)☐ None of:

       1.☐ Certified copies of the priority documents have been received.

       2.☐ Certified copies of the priority documents have been received in Application No. _____.

       3.☐ Copies of the certified copies of the priority documents have been received in this National Stage
         application from the International Bureau (PCT Rule 17.2(a)).

     * See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
     Paper No(s)/Mail Date <u>2</u>.

4) ☐ Interview Summary (PTO-413)
     Paper No(s)/Mail Date. _____ .

5) ☐ Notice of Informal Patent Application (PTO-152)

6) ☐ Other: _____.

DETAILED ACTION

1.   Claims **1-21** have been examined.

Specification

2.   The disclosure is objected because of the following informalities:

*   On page 13, starting from line 2, the term "ACE", has been mentioned, but not defined. "ACE" could be an acronym for different terms with different meaning such as "Access Control Encryption" or "Access Control Entry". It is understood and interpreted as "Access control Entry. Appropriate definition is required.

Claim Rejections - 35 USC § 112

3.   The following is a quotation of the second paragraph of 35 U.S.C 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

4.   Claim 1 is rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention. Claim 1 recites the limitation utilizing said "static maximum allowed access data" in connection with the requested permission.... There is insufficient antecedent basis for this limitation in the claim. Though, It is understood that this was intended to refer to the previously mentioned term namely "static maximum allowed access data structure", It should be corrected so that there would not be any ambiguity.

5.   Claims 2-13 depends from rejected claim 1, and includes all the limitations of the

respective claim, thereby rendering those dependent claims indefinite.

Claim Rejections - 35 USC § 103

6.   The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all

obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in
> section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are
> such that the subject matter as a whole would have been obvious at the time the invention was made to a person
> having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the
> manner in which the invention was made.

7.   **Claims 1-13** are rejected under 35 U.S.C. 103(a) as being unpatentable over the

provided Information disclosure by the applicant in particular **Netegrity white paper**,

"SiteMinder Delivers Industry-Leading Performance, Scalability, and Reliability

(hereinafter referred to as **Netegrity**) (December 1999) in view of **Schneck et al,**

(hereinafter referred as **Schneck**)(U.S. Publication Number: 2001/0021926A1)

8.   **As per claims 1, 12-14,** **Netegrity** discloses a method/a computer readable

medium for enforcing static and dynamic access policy protecting a resource in a

computer system, (Page 2, reference "Resource Cache" , under the title web Agent

Caches" and "page 3, Paragraph 1-5") (When the web agent is initialized, it

establishes or enforces a static and dynamic access policy or cache of information

protecting a resource by the web agent as explained on page 2, reference "Resource Cache " and page3, Paragraph 1-5, and page 2, last Paragraph)

- The system having a client thereof making a first access request for the resource, the method comprising: (Page 2, reference "Resource Cache" and "User session Cache")

- Determining a static maximum allowed access data structure pursuant to an evaluation of the first access request, wherein the static maximum allowed access data structure includes information representative of a set of policies that is reduced to static form that is common to a class of access requests; (Page 2, and Page 3. Paragraph 1-5)

("Applicant defined on the 1st page of the disclosure that the invention is about re-using the computations that have already been made, so that policy evaluations are not repeated, thereby making a system more efficient, freeing up computer resources and generally increasing performance. Applicant on page 3, 2nd and 3rd paragraphs, explained how several access checks involves the same user accessing resources protected by the same authorization policy and caching this particular access policy determination that is likely to be repeated called by the applicant as "static maximum allowed access" and that is granted for given access inquiry and ultimately cached. **Netegrity** on page 2, 2nd paragraph, under the title "web agent caches" discloses that the web agent has two caches to optimize performance by saving the information that is likely to be repeated on either resource or sessions cache or both. This information which is saved is interpreted by the office as "static maximum allowed access")

- Storing the static maximum allowed access data structure; (Page 2, 2nd paragraph, under the title "web agent caches") and

- In response to a determination that the static maximum allowed access data structure is applicable to a second access request, utilizing said static maximum allowed access data in connection with the requested permission set of the second access request. (Page 2, 2nd paragraph, under the title "web agent caches") (When any subsequent access or second access request is attempted/made for the resource, the web agent will determine whether the already stored "static maximum allowed access data structure" is applicable for the second or subsequent request by looking into the local memory which has already stored the information which is interpreted by the office as "the maximum allowed access data" without having to go the policy server. This optimizes performance. And on the side, after the user is authenticated, the web agent also caches the information about the user which allows second access request or subsequent operations to utilize the already stored information which is interpreted by the office as "the maximum allowed access data" either to this resources or to other resources protected by the same policies to be resulting in great optimization)

Netegrity does not explicitly teach the how "the static maximum allowed access data" is determined.

However, in the same field of endeavor, **Schneck** discloses how the access control quantities can be determined by including some items including an "allowable size of read-access to the data." (Column 14, reference [0244], and column 21, claim 20)

It would have been obvious to one having ordinary skill in the art, at the time the invention was made, to combine the techniques of determination of an allowable size as

per teachings **Schneck** in to the method of as taught by **Netegrity** in order to increase the performance and optimization of the resources.

9.   **As per claims 2 and 15,** the combinations of **Netegrity** and **Schneck** discloses a method/a computer readable medium for enforcing static and dynamic access policy protecting a resource in a computer system as applied to claim 1 and 14 above. Furthermore, **Netegrity** discloses the method wherein the storing of the static maximum allowed access data structure includes storing the static maximum allowed access data structure in cache memory. (Page 2)

10.   **As per claims 3 and 16** the combinations of **Netegrity** and **Schneck** discloses a method/a computer readable medium for enforcing static and dynamic access policy protecting a resource in a computer system as applied to claim 1 and 14 above. Furthermore, **Netegrity** discloses the method further comprising computing a client security context after the first access request for the resource is received from the client.(Page 2, paragraph 3, Under the title "user session cache ") (Client is authenticated and this meets the recitation of the limitation)

11.   **As per claims 4 and 11** the combinations of **Netegrity** and **Schneck** discloses a method/a computer readable medium for enforcing static and dynamic access policy protecting a resource in a computer system as applied to claim 1 above. Furthermore, **Netegrity** discloses the method further comprising determining whether said second access request is granted based at least in part on dynamic data and dynamic policy algorithms. (Page 3, 3rd paragraph, under the title "Authorization Cache, level 2 Policy cache ")

12.   **As per claims 5-7 and 17** the combinations of **Netegrity** and **Schneck** discloses a method/a computer readable medium for enforcing static and dynamic access policy protecting a resource in a computer system as applied to claim 1. Furthermore **Netegrity** discloses the method further comprising: evaluating whether the requested permission set

of the second access request is represented within the static maximum allowed access data

structure. (Page 2, 2nd paragraph, under the title "web agent caches") (When any

subsequent access or second access request is attempted/made for the resource, the web

agent will determine whether the already stored "static maximum allowed access data

structure" is applicable for the second or subsequent request by looking into the local

memory which has already stored the information which is interpreted by the office as "the

maximum allowed access data" without having to go the policy server, this optimizes

performance. And on the side, after the user is authenticated, the web agent also caches

the information about the user which allows second access request or subsequent

operations to utilize the already stored information either to this resources or to other

resources protected by the same policies to be greatly optimized and this meets the

recitation of this limitation)

13.   **As per claims 8-9** the combinations of **Netegrity** and **Schneck** discloses a method/a

computer readable medium for enforcing static and dynamic access policy protecting a

resource in a computer system as applied to claim 1. Furthermore **Netegrity** discloses the

method wherein evaluating whether there is at least one dynamic access control entry in a

discretionary access control list associated with the second access request.(Page 2, and Page

3, 3rd paragraph, under the title "Authorization Cache (level 2 Policy cache) (DAC or

Discretionary access control is used to control access by restricting a subject's access to an

object. The user is evaluated or authorized as explained on Page 3, 3rd paragraph, under the

title "Authorization Cache level 2 Policy cache" and this meets the recitation of the limitation)

14.   **As per claims 10** the combinations of **Netegrity** and **Schneck** discloses a method/a

computer readable medium for enforcing static and dynamic access policy protecting a

resource in a computer system as applied to claim 1. Furthermore **Netegrity** discloses the

method wherein if there is not at least one deny access control entry, the method further

comprises: evaluating whether the requested permission set of the second access request is

encompassed by (1) permissions obtained by evaluating at least one dynamic grant access

control entry and (2) permissions contained said static maximum allowed access data

structure. (Page 3, 3rd paragraph, under the title "Authorization Cache level 2 Policy cache15.")

15.   **Claims 18-21** are rejected under 35 U.S.C. 103(a) as being unpatentable over the

provided Information disclosure by the applicant in particular **Netegrity white paper**,

"SiteMinder Delivers Industry-Leading Performance, Scalability, and Reliability (hereinafter

referred to as **Netegrity**) (December 1999) in view of **Clifton,** (hereinafter referred as

Clifton)(U.S. Patent. No 5,469,556)

16.   **As per claims 18,20 and 21** **Netegrity** discloses a static maximum allowed access

        data structure stored on a computer readable medium for use in connection with access

        check determinations for an application in a computer system, the data structure

        comprising:

        •   An identifier identifying the data structure as a static maximum allowed

        access data structure; (Page 2, and Page 3. Paragraph 1-5)

        (Applicant on page 3, 2nd and 3rd paragraphs, explained how several access checks

        involves the same user accessing resources protected by the same authorization

        policy and caching this particular access policy determination that is likely to be

        repeated called by the applicant as "static maximum allowed access". This

        information "static maximum allowed access" is granted for given access inquiry

        and ultimately saving computer resources . **Netegrity** on page 2, 2nd paragraph,

under the title "web agent caches" discloses that the web agent has two caches to

optimize performance by saving the information that is likely to be repeated on

either "resource" or "sessions cache" or both. This information which is saved is

interpreted by the office as "static maximum allowed access" and this information is

identified by the Web Agent as explained on page 2.) and

• Data representing the static maximum allowed access for a given security

descriptor and a corresponding client context in connection with an access request.

(Page 2, Paragraph 3, under the title "user session cache " and Page 3. Paragraph 1-

5) (Objects stored on local computers or network has security descriptor to help

control access to the objects.Security descriptors include information about who

owns the object, who can access it and in what way. On page 2, Paragraph 3, under

the title "user session cache ", Netegrity discloses how the user is authenticated and

begin access protected resources.)

Netegrity does not explicitly teach both the identifier and the security descriptor in

resource access system.

However, in the same field of endeavor, **Clifton** discloses a resource access security

system for controlling access to resources correspondingly assigned to address in an

address spaces by the use of descriptors.(Column 3, lines 34-42; Abstract)

Furthermore **Clifton** discloses that the descriptor also includes information

identifying an address space to which resources is assigned.(Column 3, lines 31-33)

It would have been obvious to one having ordinary skill in the art, at the time the

invention was made, to combine the features of the descriptors and identification as per

teachings **Clifton** in to the method of as taught by **Netegrity** in order to secure the

system.

17.   **As per claims 19,** the combinations of **Netegrity** and **Clifton** discloses a method/a

computer readable medium for enforcing static and dynamic access policy protecting a

resource in a computer system as applied to claim 18 above. Furthermore, **Netegrity** discloses

the method wherein the storing of the static maximum allowed access data structure includes

storing the static maximum allowed access data structure in cache memory. (Page 2)

Conclusion

18.   The prior art made of record and not relied upon is considered pertinent to applicant's

disclosure. (See PTO-Form 892).

Any inquiry concerning this communication or earlier communications from the

examiner should be directed to Samson B Lemma whose telephone number is 571-272-3806.

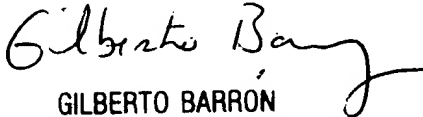The examiner can normally be reached on Monday-Friday (8:00 am---4: 30 pm).

If attempts to reach the examiner by telephone are unsuccessful, the examiner's

supervisor, BARRON JR GILBERTO can be reached on. The fax phone number for the

organization where this application or proceeding is assigned is 571-272-3799.

Information regarding the status of an application may be obtained from the Patent Application

Information Retrieval (PAIR) system. Status information for published applications may be

obtained from either Private PAIR or Public PAIR. Status information for unpublished

applications is available through Private PAIR only. For more information about the PAIR

system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private

PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

SAMSON LEMMA

S·L

12/07/2004   GILBERTO BARRON
                                              SUPERVISORY PATENT EXAMINER
                                              TECHNOLOGY CENTER 2100